Real-life Oracle E-Business Suite Security Mistakes

Stephen Kost

Chief Technology Officer
Integrigy Corporation

Session #8387

Background

Speaker

Stephen Kost

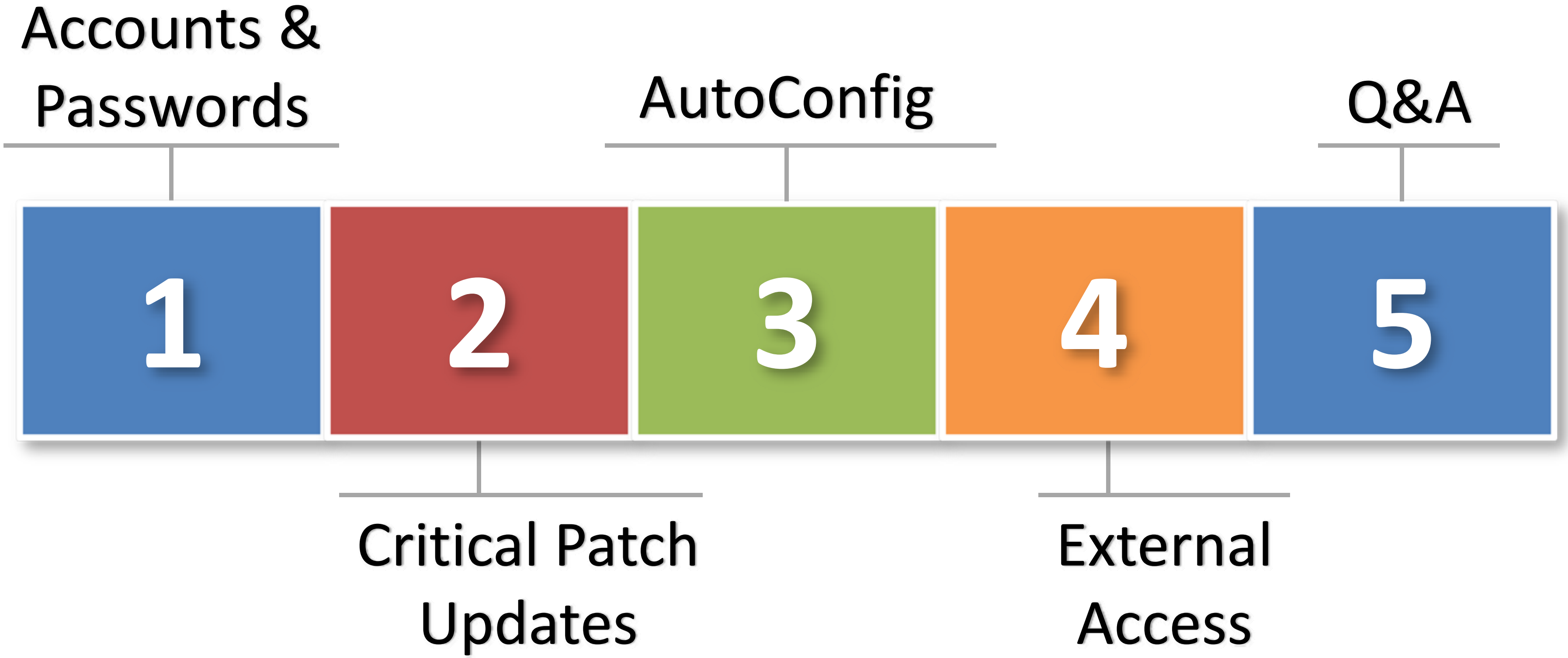
- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …

Company

Integrigy Corporation

- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

Agenda



1 Accounts & Passwords

2 Critical Patch Updates

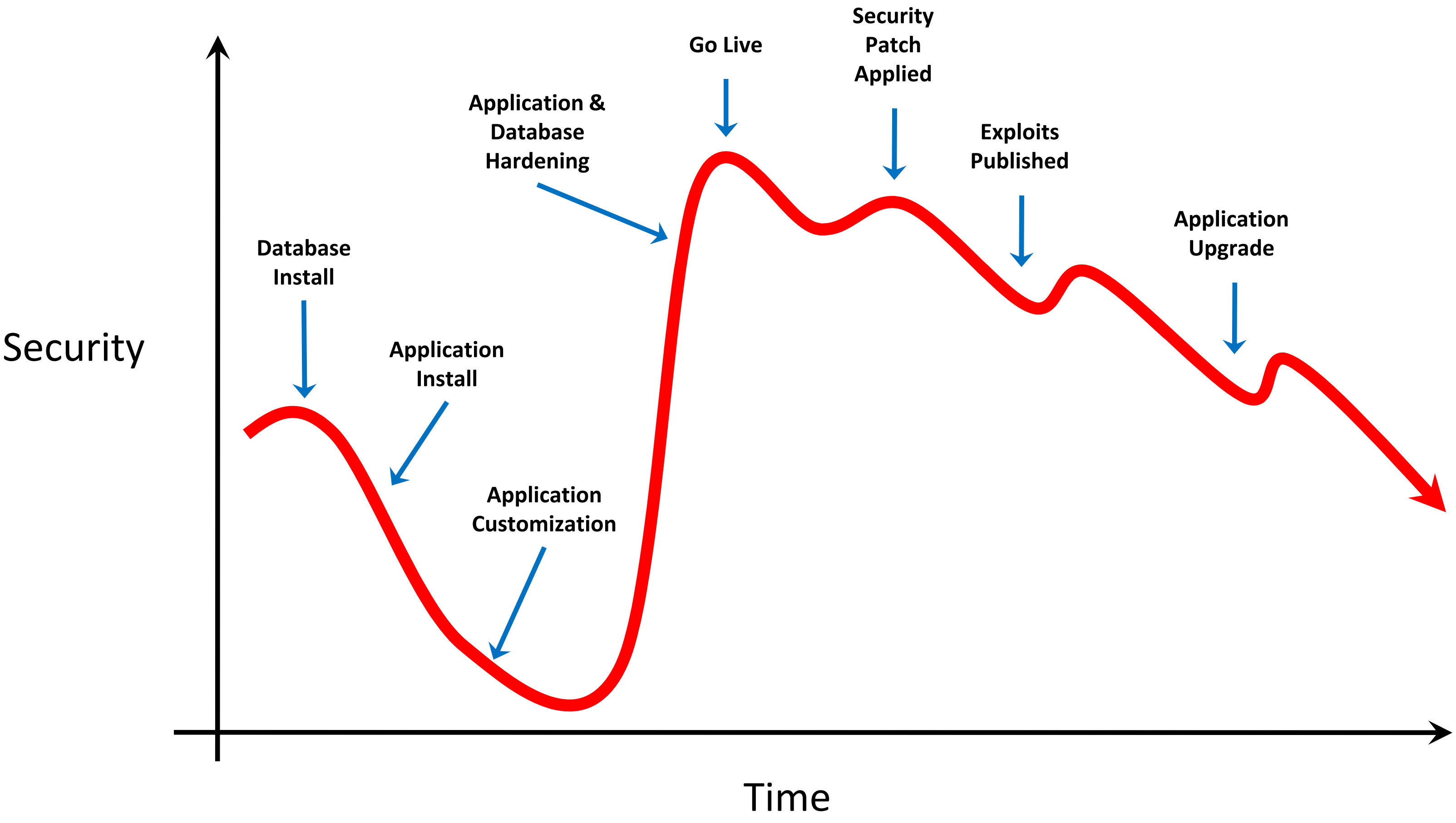
3 AutoConfig

4 External Access

5 Q&A

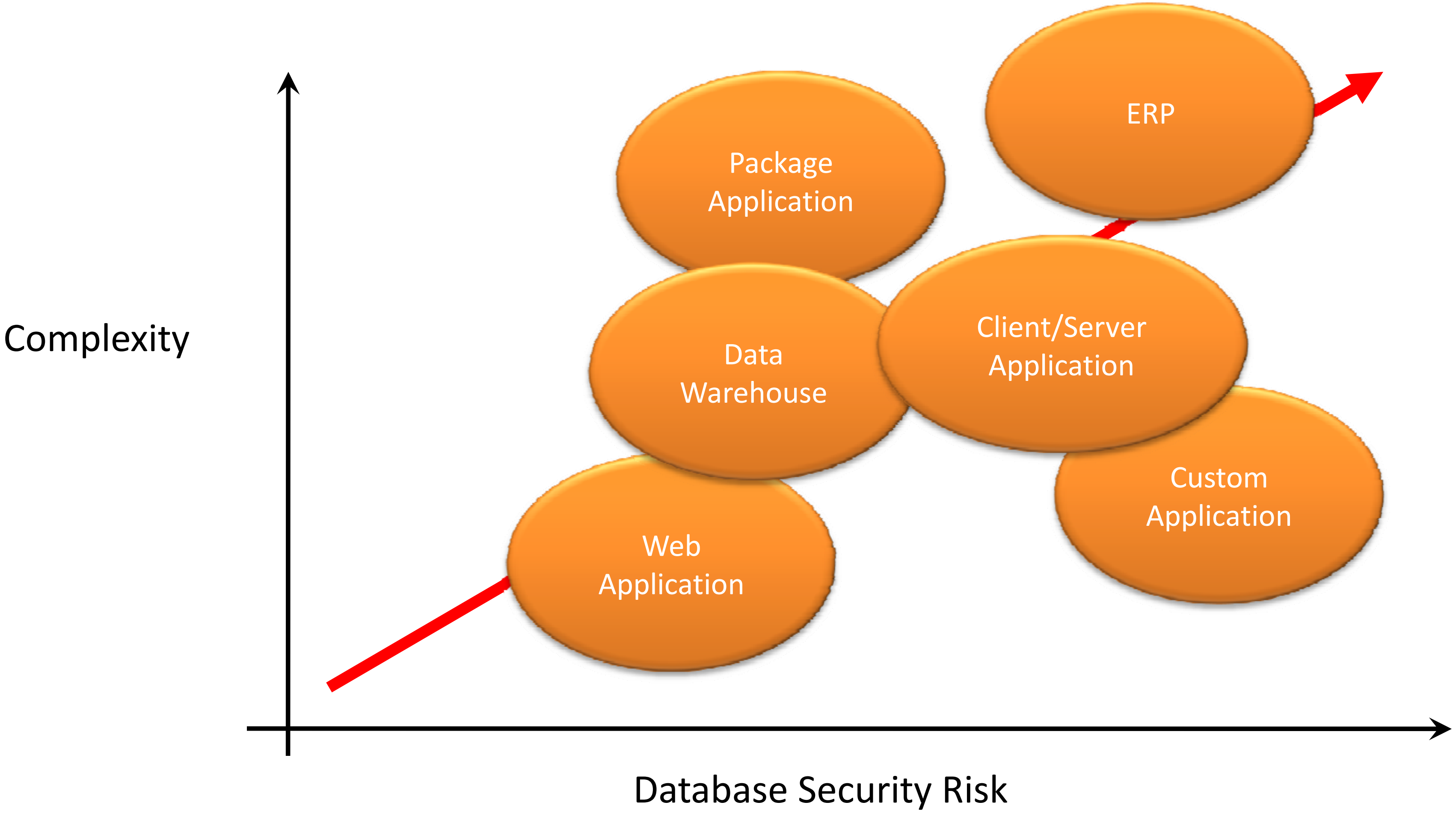
Database Security Decay

Database security decays over time due to complexity, usage, application changes, upgrades, published security exploits, etc.



Complexity and Security are Opposed

The more complex a database and application environment are, the less secure the entire environment will be.



1

Default Passwords and
More Default Passwords

1a

The completely and totally obvious answer –

You never changed the default passwords!

“How did that get reset!?”

- Default database account passwords like CTXSYS and OUTLN often “magically” get reset to default values
  - As part of application installation or maintenance (i.e., Oracle Applications)
  - As part of database maintenance (see April 2008 CPU DB13 for DBMS_STATS and OUTLN)

“I checked all the passwords!”

- **Oracle Password Scanner** only checks 683 known accounts for a single password
  - Oracle Metalink Note ID 361482.1
  - Included as part of 11g – dba_users_with_defpwd
  - Oracle’s password list has a number of important omissions/errors and does not include many common application accounts
- **Use a tool that checks all password hashes for all accounts against common dictionary words**
  - See http://www.petefinnigan.com/tools.htm for a list of password checking tools
- Use database auditing with “AUDIT USER;” to capture new database accounts and password changes

“Where did that come from!?”

- A new database account is added for each new Oracle EBS product module
  - Database accounts active with default password
  - Partial list of new module database accounts:

    CA, DDR, DNA, DPP, FTP, GMO,
    IBW, INL, IPM, ITA, JMF, MTH,
    PFT, QPR, RRS

Oracle Database Passwords

- Standard Oracle passwords are a limited character set
  - A…Z, 0…9, and _ # $
  - Passwords must start with an alpha character
  - More complex passwords can be set by enclosing the password in double quotes, however, many programs do not support these types of passwords
- Oracle Password algorithm is published on the Internet
  - Algorithm uses two cycles of DES encryption with the Username to produce a one-way hash of the password
  - Hash is unique to the username, but common across all versions and platforms of the Oracle database
  - APPS/APPS is always D728438E8A5925E0 in every database

Cracking Database Passwords

- A number of efficient and quick password cracking programs exist for Oracle
  - Speed is around 1 million passwords per second
  - Speed improvements up to 100 times due to technical advances
  - Only the hash and username are required
  - Estimated time to crack a password of x length –

Length	Permutations	Time
1	26 (26)	0 seconds
2	1,040 (26 x 39)	0 seconds
3	40,586 (26 x 39 x 39)	0 seconds
4	1,582,880	1.5 seconds
5	61,732,346	2 minute
6	2,407,561,520	40 minutes
7	93,894,899,306	1 day
8	3,661,901,072,960	42 days
9	142,814,141,845,466	1,600 days
10	5,569,751,531,973,200	64,000 days

Seeded Application Account Responsibilities

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	▪ SYSTEM_ADMINISTRATOR ▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	▪ MOBILE_ADMIN ▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	▪ ASG_MOBILE_ADMINISTRAOTR ▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	▪ OP_CUST_CARE_ADMIN
OP_SYSADMIN	OP_SYSADMIN	▪ OP_SYSADMIN
WIZARD	WELCOME	▪ AZ_ISETUP ▪ APPLICATIONS FINANCIALS ▪ APPLICATION IMPLEMENTATION

R12 Application Users Added

- New application accounts from 12.0.0 onward
  - INDUSTRY DATA
  - ORACLE12.0.0
  - ORACLE12.1.0
  - ORACLE12.2.0
  - ORACLE12.3.0
  - ORACLE12.4.0
  - ORACLE12.5.0
  - ORACLE12.6.0
  - ORACLE12.7.0
  - ORACLE12.8.0
  - ORACLE12.9.0
- All are active accounts with invalid passwords

2

Critical Patch Updates

Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-08 03.13.45.093449 PM	UPGRADE	10.2.0.3.0	Upgraded from 9.2.0.8.0
18-JAN-09 06.51.32.425375 AM	APPLY	10.2.0.4	CPUJan2009
09-APR-09 04.48.14.903718 PM	UPGRADE	10.2.0.4.0	Upgraded from 10.2.0.3.0
18-JUL-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-10 07.18.57.042620 AM	APPLY	10.2.0.4	CPUOct2010
30-OCT-10 06.42.55.108783 AM	UPGRADE	11.1.0.7.0	Upgraded from 10.2.0.4.0

What CPU Level is this database patched to?

A. January 2007

[✓ B. January 2009]

C. January 2010

D. October 2010

Database Upgrades and CPU Patches

Database Version Upgrade Patch	Latest CPU Patch Included In Upgrade Patch
9.2.0.8	July 2006
10.1.0.5	October 2005
10.2.0.3	October 2006
10.2.0.4	April 2008
10.2.0.5	October 2010
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011*

CPU Forgotten Steps

- CPU is two parts –
  - OPatch to update files in the ORACLE_HOME
  - catcpu.sql to update database objects
- Some CPUs require additional manual steps –
  - January 2008 CPU requires all views to be recompiled due view/SQL complier bugs in July 2007 CPU
- Query SYS.REGISTRY$HISTORY to verify CPU row is present
  - An indicator CPU patch was successfully applied

CPU Database Upgrades

- Scenario
  - Latest CPU patch is applied (July 2010)
  - Upgrade database to new version or patchset (9.2.0.8 to 10.2.0.4 or 10.2.0.3 to 10.2.0.4)
- Do I have to reapply the latest CPU after the database upgrade?
  - Yes, you must apply 10.2.0.4 July 2010 patch

Database Upgrades and CPU Patches

Database Version Upgrade Patch	Latest CPU Patch Included In Upgrade Patch
9.2.0.8	July 2006
10.1.0.5	October 2005
10.2.0.3	October 2006
10.2.0.4	April 2008
10.2.0.5	October 2010
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011*

CPU Application Upgrades

- Scenario
  - Latest CPU patch is applied (October 2010)
  - Upgrade application from 11.5.10.2 to 12.1.3
- Do I have to reapply the latest CPU after the application upgrade?
  - Yes, you must apply the latest 12.1.3 CPU patch

Critical Patch Updates

- R12 Critical Patch Updates are cumulative
  - 11i introduced cumulative patches with January 2010 CPU

Database Version Upgrade Patch	Included CPU
10.2.0.4	April 2008
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011

EBS Version	Included CPU
12.0.6	October 2008
12.1.1	April 2009
12.1.2	October 2009
12.1.3	January 2011*

* Estimated by Integrigy

3

AutoConfig

Security Configuration Changes

- Many security settings changes need to be made in the configuration files
  - Oracle Security Best Practices recommends changing configuration files (Metalink Note IDs 189367.1 for 11i and 403537.1 for R12)
  - Other security recommendations outline changing the configuration files directly

AutoConfig

- AutoConfig replaces almost all configuration files with new files each time it is run
  - Uses standard templates
  - Replaces placeholders in configuration file templates with settings from XML file
- Never update the configuration files directly
  - Use OAM to update AutoConfig parameters
- For custom settings, use custom files
  - Use $INST_TOP/Apache/conf/custom.conf for Apache settings

4

External Access

Oracle EBS External Access

- Oracle EBS has certified “DMZ” modules for external access
  - iStore, iSupplier, iSupport, iRecruitment, etc.
  - Only certified modules should be externally accessible
- Oracle EBS never designed as a external web application
  - All modules (250+) always installed
  - 40,000+ web pages are available even though not configured, licensed or used
  - If there is a security vulnerability, web application has access to all data

External Access Mistakes

- Configuration for external is very specific and blocks access to major parts of the application
- Must follow every step in Metalink documents 380490.1 (R12) and 287176.1 (11i)
- URL Firewall configuration is NOT optional
  - Must block access to unused web pages
  - Regular expression rules should be tested to make the rules are correct – easy to make a mistake and allow access to all pages

5

Q & A

Real-life Oracle E-Business Suite Security Mistakes   Session #8387

Stephen Kost
Chief Technology Officer
Integrigy Corporation

e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog

For information on -

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

www.integrigy.com